UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/734,102	12/11/2000	Rosario Gennaro	YOR920000597US1(13879)	3899

7590 03/29/2006

RICHARD L. CATANIA, ESQ.
SCULLY, SCOTT, MURPHY AND PRESSER
400 Garden City Plaza
Garden City, NY 11530

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/734,102	GENNARO ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-9,11-13,15 and 16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-9,11-13,15 and 16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 6 March 2006.

2. Claims 1-5, 7-9, 11-13, 15 and 16 are pending in the application.

3. Claims 1-5, 7-9, 11-13, 15 and 16 have been rejected.

4. Claims 6, 10 and 14 have been cancelled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6 March 2006 has been entered.

Response to Arguments

6. Applicant's arguments with respect to claims 1-5, 7-9, 11-13, 15 and 16 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-5, 7-9, 11-13, 15 and 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Yemini et al U.S. Patent No. 7,013,296 B1.

As to claim 1, Yemini et al discloses a method of providing anonymous digital cash, the method comprising:

providing an entity with a secure co-processor [column 13, lines 35-58];

a user establishing a secure channel to a program running on the coprocessor [column 14, lines 7-29];

the user sending a coin to be digitally signed to the coprocessor using any secure digital signature algorithm [column 28, lines 40-53];

signing the coin with a non-homomorphic signature [column 28, lines 40-53]; and

forming an encrypted copy of the signed coin and an encrypted copy of the unsigned coin using a public key of a given encryption scheme having the public key and a private key [column 30, lines 40-47];

sending back to the user both the encrypted copy of the signed coin and the encrypted copy of the unsigned coin, the user having the private key of the encryption scheme, wherein the user then using the private key to decrypt both the signed and unsigned copies of the coin, and using the pair of signed and unsigned copies of the coin as a unit as digital cash for payment to a recipient while keeping the identity of the user unknown to the coprocessor [column 30 line 62 to column 31 line 52].

As to claims 2, Yemini et al teaches a method comprising the steps of:

the processor providing a signature to authenticate [column 28, lines 40-53];

the user using the coin for payment to a merchant [column 29, lines 17-62]; and

the merchant returning the signed coin to the entity for credit to an account of the merchant [column 29, lines 17-62].

As to claim 3, Yemini et al discloses a method of creating and managing electronic cash, comprising the steps:

a customer communicating to a secure cryptography generator a given encryption scheme having a public key and a private key, and a cash amount [column 17, lines 20-27];

establishing a unit representing the cash amount [column 23, lines 15-26];

signing the unit with a non-homomorphic signature to enable the customer to use the electronic cash while keeping the identity of the customer unknown to the coprocessor [column 28, lines 40-53];

using the secure cryptography generator to encrypt both the signed unit and the unsigned unit using the public key of the encryption scheme [column 30, lines 40-47];

storing in a database the encrypted signed unit and a value for the unit [column 30, lines 40-47];

transmitting back to the customer both the encrypted copy of the signed unit and the encrypted copy of the unsigned unit [column 30 line 62 to column 31 line 52];

the customer using the private key of the encryption scheme to decrypt both the encrypted signed unit and the encrypted unsigned unit to obtain the signed unit and the unsigned unit [column 30 line 62 to column 31 line 52];

using the decrypted pair of signed and unsigned copies of the coin as a unit as a payment to a recipient [column 30 line 62 to column 31 line 52]; and

the recipient presenting the pair of signed and unsigned copies of the coin to the bank for credit [column 30 line 62 to column 31 line 52].

As to claims 4, 8 and 12, Yemini et al teaches establishing an expiration date for the unit. Yemini et al discloses storing the expiration date in the database [column 19, lines 13-15].

As to claims 5, 9 and 13, Yemini et al teaches that the signing step includes the step of using the secure cryptography generator to sign the unit [column 28, lines 40-53].

As to claim 7, Yemini et al discloses a method of creating and managing electronic cash, comprising the steps:

a secure cryptography generator, including means for receiving a given encryption scheme having a public key and a private key, and a cash amount from a customer [column 17, lines 20-27];

means for establishing a unit representing a cash amount [column 23, lines 15-26];

means for signing the unit with a non-homomorphic signature to enable the customer to use the electronic cash while keeping the identity of the customer unknown to the coprocessor [column 28, lines 40-53];

wherein the secure cryptography generator encrypts both the signed unit and the unsigned unit using the public key of the encryption scheme [column 28, lines 40-53];

a database for storing the encrypted signed unit and a value for the unit [column 30, lines 40-47];

means for transmitting back to the customer both the encrypted copy of the signed unit and the encrypted copy of the unsigned unit [column 30 line 62 to column 31 line 52];

means for the customer using the private key of the encryption scheme to decrypt both the encrypted signed unit and the encrypted unsigned unit to obtain the signed unit and the unsigned unit, wherein the customer then uses the pair of the signed and unsigned copies of the coin as a unit as a payment to a recipient [column 30 line 62 to column 31 line 52].

As to claim 11, Yemini et al discloses a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for creating and managing electronic cash, said method steps comprising:

using a secure cryptography generator to receive from a customer a given encryption scheme having a public key and a private key, and a cash amount [column 17, lines 20-27];

establishing a unit representing the cash amount [column 23, lines 15-26];

signing the unit with a non-homomorphic signature to enable the customer to use the electronic cash while keeping the identity of the customer unknown to the coprocessor [column 28, lines 40-53];

using the secure cryptography generator to encrypt both the signed unit and the unsigned unit using the public key of the encryption scheme [column 28, lines 40-53];

storing in a database the encrypted signed unit and a value for the unit [column 30, lines 40-47];

transmitting back to the customer both the encrypted copy of the signed unit and the encrypted copy of the unsigned unit [column 30 line 62 to column 31 line 52];

the customer using the private key of the encryption scheme to decrypt both the encrypted signed unit and the encrypted unsigned unit to obtain the signed unit and the unsigned unit;

using decrypted pair of the signed and unsigned copies of the coin as a unit as a payment to a recipient [column 30 line 62 to column 31 line 52]; and

the recipient presenting the pair of singed and unsigned copies of the coin to the bank for credit [column 30 line 62 to column 31 line 52].

As to claim 15, Yemini et al teaches a method, wherein:

the communicating step includes the step of the customer sending to the generator the public key of the encryption scheme [column 28, lines 40-53]; and

the step of using the secure cryptography generator includes the step of using the public key to encrypt the signature on the unit [column 28, lines 40-53].

As to claim 16, Yemini et al discloses that:

the signing step includes the step of using a non-homomorphic signature scheme to sign the unit [column 28, lines 40-53];

the non-homomorphic signature scheme includes a private key and a public key [column 28, lines 40-53]; and

the step of using the non-homomorphic signature scheme includes the step of using the private key of the non-homomorphic signature scheme to sign the unit [column 28, lines 40-53].

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy AKM
March 20, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER
CR 3/26/06